Vulnerability Management Session Report

It was standing room only at the Gartner IT Security Summit session "New Technologies in Vulnerability and Patch Management" last week where Mark Nicolett, a Gartner Research VP rounded out the vulnerability management landscape. An information hungry crowd took copious notes as Mr. Nicolett defined vulnerability management and its components, and offered guidance for evaluating threats, quantifying business risk and eliminating vulnerabilities using process and technology.

"Vulnerabilities", Nicolett said, "are weaknesses in process, administration or technology that can be exploited to compromise IT security." They can be "present in any layer of the application stack, and can be caused by weaknesses in just about every IT administration, process or design function".

He defined Vulnerability Management as an integration of processes and technologies that enable an organization to proceed along six steps.

The first step is to Baseline and Discover. He urged using both a bottom up (known vulnerabilities) and top down (security configuration policies) approach to achieving your baseline. Risk then needs to be determined and by bringing together vulnerability data, threat data and asset classification. A set of mitigation priorities can then be established.

Next step: shield and mitigate to defend against potential exploit of high priority vulnerabilities. You then need controls that can eliminate vulnerabilities and root causes that often exist because of improper system configuration, inadequate user policy, or lack of change management. According to Mr. Nicolett, "Eliminating a vulnerability is important, but eliminating the root cause will prevent the reintroduction of vulnerabilities that have been solved.

Though there is much attention in recent months about patch management, Mr. Nicolett's presentation made it clear that patching is but a component of vulnerability management or what is increasingly referred to as "configuration management." Mr. Nicolett recommends using configuration and patch management tools in concert. A convergence of sorts is occurring as the traditional configuration management vendors are including patch management features and functionality while patch management vendors are entering the configuration management space.

But whether missing patch or improper configuration, the time between knowledge of a vulnerability and realization of a threat is becoming shorter. Changes require testing and worms have been appearing in as little as a week after publication of a vulnerability. "Therefore, it is necessary to shield vulnerable systems until the vulnerability is mitigated." Nicolett said, and he recommends using "Scan and Block" tools and processes designed to temporarily shield vulnerable systems.

Because no vendor provides a single or well-integrated suite of products, Gartner does not yet recognize "vulnerability management" as fitting its definition of a market. Mr. Nicolett's slides were chock full of point solution vendors and he said that a few are coming close to an integrated solution. He also called for vulnerability management technologies to enable a system of workflow as part of their solution. He believes that some components of vulnerability management should be centralized and others not. It is important that active vulnerability and compliance monitoring be centralized and that many mitigation tasks are not.

It’s the “classic security challenge" according to Mr. Nicolett. "The scope of the problem greatly exceeds the span of control of the security professional". Security professionals rely on the cooperation of other in house IS personnel or contractors to effect a change. These folks do not usually have the same perspective and priorities. As this dynamic tends to help lengthen the mitigation process, it reinforces Nicolett's belief that effective "scan and block technologies be deployed.

With so many components of vulnerability management and technologies available, where does one begin? Mr. Nicolett suggests starting with perimeter configurations, gaining the ability to deploy patches rapidly and installing personal firewalls.